Franklin T9 (r717) 4G Hotspot

| [user](http://192.168.0.1/) | [hidden](http://192.168.0.1/hidden/) | [webpst](http://192.168.0.1/webpst/) | [itadmin](http://192.168.0.1/itadmin/) | [engineering](http://192.168.0.1/engineering/franklin/) | | ssh |
| --- | --- | --- | --- | --- | --- | --- |
| [user set] | frk@r717 | frk@r717 | t9\_it\_@dmin | r717 | frkengr717 | frk9x07 |

| **WARNING** Upon reception of a Franklin T9 4G Hotspot (r717), it is imperative that it is not allowed to access the internet until the self update mechanism has been disabled. **Do not insert an active sim card into the device until the self update mechanism has been disabled.** In the event of updating to the latest locked firmware, see [downgrade guide](https://snt.sh/2021/09/rooting-the-t-mobile-t9-franklin-wireless-r717-again/) at risk of bricking. |
| --- |

The r717 is linux based, sim unlockable, IMEI alterable, SSH root accessible, band lockable (2,4,5,12,25,26,41,66,71), and provides 2 MIMO TDD, 2 MIMO FDD, and 1 WIFI external antenna connections that are user accessible. WIFI supports up to 15 devices via B,G,N 2.4GHz & N,AC 5.0GHz and USB 2.0 tethering. The device can function without battery powered solely by USB type A-micro cable and includes a small LCD screen, power/menu button, and reset button. The r717 runs Linux 3.18 on an ARMv7 Processor rev 5 (v7l) with 256 MB RAM, 256 flash and connects via a Qualcomm [MDM9207-0](https://www.t-mobile.com/content/dam/tfb/pdf/tfb-iot/MDM9207-1%20IoT%20Chipset.pdf) modem and microsim under the battery. The 2450 mAh lithium battery provides about two days of uptime depending on tower reception.

The board sports several additional connectivity features, including several labeled terminals in two groups:

GND, UART RX, UART TX, 1v8, RST, TDO, TCK, TMS, TDI, TRST

GND, USB\_HS\_DP, USB\_HS\_DM, VSYS, VBUS, BAT\_TEMP

Antenna ports are labelled:

WIFI\_2.4G/5G, TDD\_Main, TDD\_Div, FDD\_Main, FDD\_Div

All firmware versions are hosted at <https://mega.nz/folder/FJ8wWYAJ#Q1oUEtIUJrtjB1atkOAXrA>

**Firmwares after 891 are less friendly.**

| contents  [**basic unix terminal commands**](#_oa2iz6ligcnv)  [**basic unix terminal keyboard shortcuts**](#_mj0wex19em80)  [**secret pages access & contents**](#_4iddllq6csjm)  [**disable self update mechanism**](#_hhhwm4ciu3v7)  [**TTL modification**](#_dtxtot3goyr5)  [**digesting iptables mangle command**](#_4myr0h27skfb)  [**checking on active iptables rules**](#_q2g0tqf1ppdj)  [**Windows vs Unix line endings**](#_vhd15goqylgm)  [**Windows Powershell desktop shortcut to execute SSH reboot**](#_tzyn1q3btedr)  [**sources & additional info**](#_d458y9rnwohw) |  |
| --- | --- |

Note: This document was crafted around running the following commands using the command line interface client cmder on Windows. There are issues when copying and pasting these commands, such as quotation marks sometimes needing to be reapplied manually otherwise causing the command to fail, or a text document end of line formatting difference between operating systems. Simply because a command fails on initial attempt after pasting does not mean the command itself is necessarily incorrect, but there may be some nonobvious deeper confusion occurring.

Quick Setup

| 1 | carrier unlock / sim unlock |
| --- | --- |
| * get imei from: <http://192.168.0.1/about/> * enter into script: <https://jsfiddle.net/4zds6531/> * enter into settings: <http://192.168.0.1/settings/mobile_network-sim.html>   !!! factory reset via bottom button relocks the factory sim lock | |
| 2 | downgrade firmware to 891 |
| | from 1311 | | --- | | * plug device in with a fully charged battery * download 891 from: <https://mega.nz/folder/FJ8wWYAJ#Q1oUEtIUJrtjB1atkOAXrA> * apply in settings: <http://192.168.0.1/settings/device-software_update.html> * wait until device reboots again on its own |  | from 2602 | | --- | | * plug device in with a fully charged battery * confirm internet connectivity using an active sim by connecting as a wifi client * apply file: <https://snt.sh/uploads/t9/configs/downgrade_2602_to_891_config.bin>   to interface at: <http://192.168.0.1/settings/device-backup_and_restore.html>   * after device reboots, if needed, enter APN for device to download downgrade file * wait until device reboots again on its own   \*\*\* this process automatically disables the automatic update mechanism | | |
| 3 | disable automatic update |
| * apply false update URL at: <http://192.168.0.1/webpst/fota_test.html>   password: frk@r717  false address: https://no.more.updates.thanks.com | |
| 4 | imei |
| * imei generator: <https://www.imei.info/services/imei_generator/Motorola/check-free/?input=359517092814730> * imei and mac address: <http://192.168.0.1/engineering/franklin/imei_mac.html>   user: r717  password: frkengr717 | |
| 5 | TTL |
| * turn SSH on: <http://192.168.0.1/webpst/service_setting.html>   user: root  password: frkengr717   * place *file set\_ttl* on desktop * run commands to move via ssh:   <https://cmder.app/>   | *scp "C:/%HOMEPATH%/Desktop/set\_ttl" root@192.168.0.1:/etc/init.d/*  password: frk9x07  *ssh root@192.168.0.1*  *chmod 755 /etc/init.d/set\_ttl*  *cd /etc/rc5.d/; ln -s ../init.d/set\_ttl S99set\_ttl*  sed -i -e 's/\r//g' /etc/init.d/set\_ttl  *reboot*  iptables -L PREROUTING -t mangle  iptables -L POSTROUTING -t mangle  ip6tables -L PREROUTING -t mangle  ip6tables -L POSTROUTING -t mangle | | --- | | |
| 6 | settings |
| * wifi settings: <http://192.168.0.1/settings/wifi-basic.html> * always on: <http://192.168.0.1/settings/wifi-advanced.html> * disable LED: <http://192.168.0.1/settings/device-preferences.html> * UPnP & DNS: <http://192.168.0.1/settings/advanced_router-dns_mode.html> * APN: <http://192.168.0.1/settings/mobile_network-apn.html> | |

Verbose Instructions

| basic unix terminal commands using <https://cmder.net/> for SSH terminal access | | ssh root@192.168.0.1 | log in to device at specified address using *root* account  password: frk9x07 | | --- | --- | | cd [directory] | change to top level directory | | cat [file] | read small text file to screen  /var/log/boot  /etc/init.d/set\_ttl  /etc/rc5.d/ | | less [file] | real large text file to screen   * search with / and enter | | clear | removes terminal contents | | ls | list directory contents | | ls -l [file] | check file permissions | | reboot | reboots logged in device | | exit | closes connection and terminal | | scp [OPTION] [user@]SRC\_HOST:]file1 [user@]DEST\_HOST:]file2 | move a file over ssh from source to destination; local command ran from client not logged into SSH | | ifconfig | displays details about all network interfaces | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| basic unix terminal keyboard shortcuts | | ctrl + z | cancels current operation or moves it to the background  (sends a TSTP **t**emporary **st**o**p** signal to request it to stop temporarily) | | --- | --- | | ctrl + c | cancels current operation  (sends a [SIGINT](https://www.computerhope.com/jargon/s/sigint.htm) signal, which cancels or terminates the currently-running program) | |
| secret pages access & contents Hidden Configuration Pages   * <http://192.168.0.1/hidden/> * <http://192.168.0.1/webpst/>   Password: frk@r717  Password was extracted from /var/volatile/www/htdocs/cgi-bin/login.cgi  IT Admin Page   * <http://192.168.0.1/itadmin/> * Password: t9\_it\_@dmin   Password was extracted from /var/volatile/www/htdocs/cgi-bin/login.cgi  Hidden Engineering Page   * <http://192.168.0.1/engineering/franklin/> * Username: r717 * Password: frkengr717   User and Password were extracted from /etc/pwlighttpd  Note: On firmwares newer than 891, you need to first run the following as root before you can access the engineering pages.   | /usr/bin/copy\_htdocs.sh eng | | --- |  | Hidden  - LTE band configuration including activation and priority  - detailed APN profile configuration  - IMEI and service status  ITAdmin  - WIFI mac address whitelisting  - WIFI configuration  - Web interface configuration, including disabling web panel access  - backup and restore configuration, and factory reset  Engineering Page  - update firmware  - enable SSH  - alter IMEI & MAC address  - factory reset and factory reset with permanent data  - select operator target (?)  - reboot | | --- | | |
| disable self update mechanism two methods, the first very easy, the second providing insight on file structure & contents:  method 1:  go to <http://192.168.0.1/webpst/fota_test.html>  change update URL to a fake URL  **REBOOT THE DEVICE OR IT WILL UPDATE!!!**  method 2:  alter the file  */data/configs/mobileap\_cfg.xml*  change lines 355 to 360 from:   | <UpdateFromServer>  <Enable>1</Enable>  <CheckUrl>https://fota.pintracview.com/fota/T9/check\_update.php</CheckUrl>  <RetryInterval>300</RetryInterval>  <NextCheckInterval>172800</NextCheckInterval>  </UpdateFromServer> | | --- |   to   | <UpdateFromServer>  <Enable>0</Enable>  <CheckUrl>https://notarealdomain.com/noupdatesforyou</CheckUrl>  <RetryInterval>300</RetryInterval>  <NextCheckInterval>172800</NextCheckInterval>  </UpdateFromServer> | | --- |   reboot  **REBOOT THE DEVICE OR IT WILL UPDATE!!!**  a summarized list of commands:   | *scp root@192.168.0.1:/data/configs/mobileap\_cfg.xml "%HOMEPATH%/Desktop/"*  password: frk9x07  **ALTER FILE**  *scp "%HOMEPATH%/Desktop/mobileap\_cfg.xml" root@192.168.0.1:/data/configs/*  *ssh root@192.168.0.1*  *reboot* | | --- | | |
| sim unlock Two methods: the first is a tool created for this purpose, the second is the same done manually  Method 1: <https://jsfiddle.net/4zds6531/>  Method 2:  To generate your SIM unlock code, execute the following in any Linux or Mac terminal or on the website [Linux Online Terminal](https://cocalc.com/doc/terminal.html).   | *export IMEI=YOURIMEIGOESHERE*  *echo -n "${IMEI}simlock" | sha1sum | cut -c1-8* | | --- |   Notes  - resetting the device sim relocks the device, so save your unlock code  - changing the IMEI of the device requires a new unlock code | |
| TTL modification place the following file in  */etc/init.d/set\_ttl*  Note: Windows standard text editors use different line endings than Unix  In [Notepad++](https://notepad-plus-plus.org/downloads/) go to *Edit >> EOL Conversion >> Unix (LF)* to save a unix compatible file, or edit it on Windows, upload, and run the command at the end of this document titled “Windows vs Unix line endings” to fix all the line endings   | *set\_ttl* | | --- | | #!/bin/bash  ### BEGIN INIT INFO  # Provides: ttl  # Required-Start: $remote\_fs $syslog $networking  # Required-Stop: $remote\_fs $syslog  # Default-Start: 2 3 4 5  # Default-Stop: 1  # Short-Description: Set TTL in iptables  ### END INIT INFO  TTL=65  INTERFACE=rmnet\_data0  case "$1" in  start)  echo "Setting TTL on $INTERFACE to $TTL..."  ip6tables -t mangle -I POSTROUTING -o $INTERFACE -j HL --hl-set $TTL  ip6tables -t mangle -I PREROUTING -i $INTERFACE -j HL --hl-set $TTL  iptables -t mangle -I POSTROUTING -o $INTERFACE -j TTL --ttl-set $TTL  iptables -t mangle -I PREROUTING -i $INTERFACE -j TTL --ttl-set $TTL  ;;  \*)  echo "$1 is not implemented"  ;;  esac  exit 0 |   then run   | *chmod 755 /etc/init.d/set\_ttl* | | --- | | *cd /etc/rc5.d/; ln -s ../init.d/set\_ttl S99set\_ttl* | | *reboot* |   a summarized list of commands **with file *set\_ttl* on Windows desktop**:   | *scp "C:/%HOMEPATH%/Desktop/set\_ttl" root@192.168.0.1:/etc/init.d/*  password: frk9x07  *ssh root@192.168.0.1*  *chmod 755 /etc/init.d/set\_ttl*  *cd /etc/rc5.d/; ln -s ../init.d/set\_ttl S99set\_ttl*  *reboot* | | --- | | |

| digesting iptables mangle command iptables -t mangle -I POSTROUTING -o $INTERFACE -j TTL --ttl-set $TTL  <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-en-4/s1-iptables-options.html>  iptables [-t <table-name>] <command> <chain-name> <parameter-1> \ <option-1> <parameter-n> <option-n>  -t mangle specifies that the table *mangle* is being worked on  -I specifies insertion location on chain  POSTROUTING applies rule in *POSTROUTING* chain  -o specifies outgoing interface - interface list available using *ifconfig* |
| --- |
| checking on active iptables rules The following command lists all active rules under a specified chain/table category and thus can be used to check whether an *iptables* rule is active:  iptables -L <chain> -t <table>  iptables -L PREROUTING -t mangle  iptables -L POSTROUTING -t mangle  ip6tables -L PREROUTING -t mangle  ip6tables -L POSTROUTING -t mangle |
| Windows vs Unix line endings Carriage return characters inserted by Windows text editors will cause script to fail. The following command removes those characters:  sed -i -e 's/\r//g' /etc/init.d/set\_ttl |

| Windows Powershell desktop shortcut to execute SSH reboot Run in an administrator level powershell terminal: Set-ExecutionPolicy Unrestricted  Download & install *plink.exe*: <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>  Place *T9 reboot.ps1* on the desktop. Create a shortcut with the target *T9 reboot shortcut* on the desktop.  Note: The device this shortcut is run from must have logged in manually once via SSH to confirm the server identity.   | *T9 reboot(shortcut)* | | --- | | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command "& '%HOMEPATH%/Desktop/T9 reboot.ps1' " |  | *T9 reboot.ps1* | | --- | | Param (  [string]$server = "192.168.0.1" ,  [string]$login = "root" ,  [string]$key,  [string]$pw = "frk9x07",  [string]$script,  [string]$cmd = "reboot",  [switch]$batch = $false,  [switch]$agentForwarding = $true,  [switch]$verbose = $false,  [switch]$acceptHostKey = $true # For convenient. Make sure the server is the computer you think it is.  )  $scriptPath = Split-Path -Parent $MyInvocation.MyCommand.Path  $plinkPath = Join-Path -Path $scriptPath -Childpath "Plink.exe"  if (-not (Test-Path $plinkPath)){  Throw "Missing Plink.exe in script path. Please download it from http://the.earth.li/~sgtatham/putty/latest/x86/plink.exe"  }  if ($key -eq "" -and $pw -eq "") {  Throw "You must supply either a password or key file."  }  if ($script -eq "" -and $cmd -eq "") {  Throw "You must supply either a shell script file or command."  }  if ($key -ne "" -and $pw -ne "") {  Write-Output "Notice: Only password or key file is required. Using key file."  }  if ($script -ne "" -and $cmd -ne "") {  Write-Output "Notice: Only script file or command is required. Using script file."  }  if ($acceptHostKey -eq $true) {  $command = "echo Y|" + $plinkPath  } else {  $command = $plinkPath  }  $command += " -ssh " + $server + " -l " + $login  if ($key -ne "") {  $command += " -i " + $key  } else {  $command += " -pw " + $pw  }  if ($batch -eq $true) {  $command += " -batch"  }  if ($agentForwarding -eq $true) {  $command += " -a"  }  if ($verbose -eq $true) {  $command += " -v"  }  if ($script -ne "") {  $command += " -m " + $script  } else {  $command += ' "' + $cmd + '"'  }  $command += " 2>&1"  if ($verbose -eq $true) {  Write-Output "Command to Plink:"  Write-Output $command # Write out the command for debugging  Write-Output ""  }  $output = Invoke-Expression $command  if ($LastExitCode -ne 0) {  Throw $output  } else {  Write-Output $output  Exit 0  } | |
| --- | --- | --- | --- | --- |

| sources & additional info | |
| --- | --- |
| founding article on hacking this device | <https://snt.sh/2020/09/rooting-the-t-mobile-t9-franklin-wireless-r717/> |
| article on downgrading from the undesirable most recent firmware | <https://snt.sh/2021/09/rooting-the-t-mobile-t9-franklin-wireless-r717-again/> |
| init.d rc.d script for running TTL modifying commands at boot | <https://gist.github.com/weirded/f49ac134aecbd32b71ab22619c7496ab> |
| T9 additional fine details and images | <https://robpol86.com/franklin_t9.html> |
| T-Mobile Franklin T9 tech specs site | <https://www.t-mobile.com/support/devices/mobile-internet/franklin-9-mobile-hotspot/tech-specs-franklin-t9-mobile-hotspot> |
| Use Powershell to connect to a remote server via SSH and run a shell script/command | <https://gist.github.com/sveinn-steinarsson/f8d21f1832800bd4428a> |
| powershell script via shortcut | <https://stackoverflow.com/questions/10137146/is-there-a-way-to-make-a-powershell-script-work-by-double-clicking-a-ps1-file> |
| antenna connectors (MS-162) | <https://old.reddit.com/r/Calyx/comments/l470a9/franklin_t9_says_no/gyh6dr5/> |

<https://sigquit.wordpress.com/2012/08/20/an-introduction-to-libqmi/>